Datenschutzgesetz (1/2)

Das Parlament hat das neue Datenschutzgesetz seit längerem verabschiedet. Das totalrevidierte Datenschutzgesetz (DSG) und die Ausführungsbestimmungen in der neuen Datenschutzverordnung (DSV) und der neuen Verordnung über Datenschutzzertifizierungen (VDSZ) treten am 1. September 2023 in Kraft. Die Unternehmen müssen sich ab dem 1. September 2023 an die revidierten Regelungen anpassen.

Die wichtigsten Neuerungen im Überblick:

- **Kein Schutz mehr von Daten jur. Personen**: Künftig werden nur noch natürlich Personen geschützt werden, während jur. Personen (z.B. AG, GmbH etc.) sich für ihren Schutz nicht mehr auf das revDSG berufen können. Ihnen verbleibt der Schutz durch das Firmenrecht sowie weitere Bestimmungen (z.B. Persönlichkeitsschutz nach ZGB, UWG).
- **Als besonders schützenswerte Daten**
  Die Auflistung der besonders schützenswerten Personendaten wird um genetische Daten sowie um biometrische Daten (z.B. Fingerabdruck oder Retina-Scan) erweitert.
- **Profiling mit hohem Risiko – nur mit Einwilligung**
  Unter Profiling wird jede Art der automatisierten Bearbeitung von Personendaten verstanden, mit welcher bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen (z.B. Arbeitsleistung, wirtschaftliche Situation, Gesundheit, Interessen, Aufenthaltsort), bewertet, analysiert oder vorhergesagt wird. Verschärfte Rechtsfolgen gelten indes nur beim Profiling mit hohem Risiko für die Persönlichkeit der betroffenen Person. Ein Beispiel dafür wäre, wenn über Monate hinweg ein unternehmensinternes System Daten über einen Mitarbeiter sammelt – insbesondere Leistungsdaten. Mithilfe dieser Informationen erstellt dieses System ein Profil und wertet es zum Termin des nächsten Feedback-Gesprächs aus. Anschließend entscheidet es selbständig, ob dem Mitarbeiter eine Gehaltserhöhung gewährt wird oder nicht. Die Personen, die das Feedback-Gespräch führen, sind lediglich berechtigt, dem Mitarbeiter das Ergebnis mitzuteilen, ohne zuvor Einfluss auf den Entscheidungsprozess gehabt zu haben.
- **Auftragsbearbeiter**: Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung an einen Auftragsbearbeiter (Outsourcing z.B. die Cloud) übertragen werden wenn. Der Auftragsbearbeiter hat die Daten gleich zu bearbeiten wie der Verantwortliche. Der Verantwortliche hat sich dabei zu vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.
- **Ausbau Auskunftspflichten:** Betroffene Personen haben neu Anspruch auf jede Information, welche für sie erforderlich ist, um ihre Rechte nach dem revDSG geltend zu machen. Die Auskunft ist daher nicht auf die abschliessend definierten Mindestinformationen (worunter neu auch Angaben über Aufbewahrungsdauer, Auslandtransfers und automatisierte Einzelentscheide fallen) beschränkt.
- **Recht auf Datenübertragbarkeit:** Mit dem Recht auf Datenherausgabe und Datenübertragung (Datenportabilität) kann die betroffene Person kostenlos vom Verantwortlichen die Herausgabe ihrer Personendaten bzw. deren Übertragung an einen anderen Verantwortlichen in maschinenlesbarer Form verlangen.

Datenschutzgesetz (2/2)

Welche Pflichten ergeben sich unter dem neuen Datenschutzgesetz für Ihr Unternehmen?

- **Sicherstellung von Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen:**
  Der Verantwortliche muss die Datenbearbeitung von Personendaten ab der Planung so gestalten, dass die Datenschutzvorschriften und insbesondere die Bearbeitungsgrundsätze eingehalten werden (Privacy by Design). Weiter müssen die Voreinstellungen so eigenstellt sein, dass die Bearbeitung von Personendaten auf das für den Verwendungszweck notwendige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt. (Privacy by Default) / (Art. 7 revDGS).
- **Verzeichnis der Datenbearbeitungstätigkeiten:** Verantwortlicher und Auftragsbearbeiter führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten. Eine Ausnahme gilt allerdings für Unternehmen, welche weniger als 250 Mitarbeitenden, allerdings nur dann, wenn deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt.

  Das Verzeichnis muss diverse Angaben enthalten wie bspw. Identität des Verantwortlichen, Bearbeitungszweck, Empfängerinnen und Empfänger, Aufbewahrungsdauer der Personendaten, Angaben über allfällige Datentransfers ins Ausland etc. (Art. 12 revDSG).
- **Meldepflicht bei Verletzungen des Datenschutzes:** Es besteht eine Meldepflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sowie gegenüber der betroffenen Person im Fallen einer Datensicherheitsverletzung. (Art. 24 revDGS).
- **Datenschutz-Folgenabschätzung:** Die Verpflichtung, in bestimmten Fällen eine Folgenabschätzung zum Schutz der Personendaten durchzuführen, wenn aufgrund einer Bearbeitung ein hohes Risiko besteht (Art. 22 revDSG).
- **Erweiterte Informationspflichten:** Die Informationspflicht bei der Datenerhebung und die Pflicht zur Nennung des/der Staates/Staaten im Falle eines Transfers ins Ausland (Art. 19 revDSG). Hier ist das revDSG ausnahmsweise strenger als die heute gültige DSGVO.
- **Automatisierte Einzelfallentscheidung:** Die Informationspflicht im Falle einer automatisierten Einzelentscheidung - d.h. einer Entscheidung, welche in Bezug auf eine Person mit Hilfe von Algorithmen getroffen und auf ihre persönlichen Daten angewendet werden, ohne dass ein Mensch in den Prozess eingreift (Art. 21 revDSG).

Mögliche Sanktionen: Verantwortliche Personen können bei vorsätzlicher Verletzung der Informations- und Auskunftspflichten sowie der Sorgfaltspflichten neu mit Busse bis CHF 250'000 bestraft werden. Ausreichend ist der Eventualvorsatz, weshalb die Strafbarkeit bereits gegeben ist, wenn eine tatsächlich eingetretene Verletzung in Kauf genommen wurde. Dies führt dazu, dass nach dem revidierten DSG Verantwortliche im Unternehmen wie CEOs, CIOs oder andere Funktionen direkt sanktioniert werden können. Die Zuständigkeit liegt dabei bei den kantonalen Staatsanwaltschaften.